

High-rate self-synchronizing codes

Yuichiro Fujiwara, *Member, IEEE*, and Vladimir D. Tonchev

Abstract—Self-synchronization under the presence of additive noise can be achieved by allocating a certain number of bits of each codeword as markers for synchronization. Difference systems of sets are combinatorial designs which specify the positions of synchronization markers in codewords in such a way that the resulting error-tolerant self-synchronizing codes may be realized as cosets of linear codes. Optimal difference systems of sets are those that sacrifice as few bits as possible for a given code length, alphabet size, and error-tolerance capability. However, it seems difficult to attain optimality with respect to known bounds when the noise level is relatively low. In fact, the majority of known optimal difference systems of sets are for exceptionally noisy channels, requiring a substantial amount of bits for synchronization. To address this problem, we present constructions for difference systems of sets that allow for higher information rates while sacrificing optimality to only a small extent. Our constructions utilize optimal difference systems of sets as ingredients and, when applied carefully, generate asymptotically optimal ones with higher information rates. We also give direct constructions for optimal difference systems of sets with high information rates and error-tolerance.

Index Terms—Synchronization, self-synchronizing code, comma-free code, redundancy, difference system of sets, cyclotomy.

I. INTRODUCTION

A *self-synchronizing code* is a block code where the symbol string formed by an overlapped portion of any two concatenated codewords or a portion of any single codeword is not a valid codeword. In the coding theory literature, self-synchronizing codes are also called *comma-free codes*. The property that no codeword appears as a substring of two adjacent codewords allows for synchronization without any external help or separate clock signal. Carefully designed self-synchronizing codes may be used for synchronization under the presence of additive noise as well.

Self-synchronizing codes are also of interest from mathematical viewpoints and have been investigated in both coding theory and combinatorics. This paper focuses on a mathematical approach to the construction of self-synchronizing codes of high information rate by using combinatorial designs.

A *splice* of two codewords x and y is a concatenated sequence of length v composed of the last i bits of x and the first $v - i$ bits of y for some positive integer $i \leq v - 1$.

A code C is *comma-free* with index ρ if the Hamming distance between any codeword z and any splice of any two codewords x, y is at least ρ .

The first author acknowledges support from JSPS Postdoctoral Fellowships for Research Abroad. Vladimir Tonchev acknowledges the support by an NSA Grant. The material in this paper was presented in part at the International Symposium on Information Theory and its Applications, Honolulu, HI USA, October 2012.

Y. Fujiwara and V. D. Tonchev are with the Department of Mathematical Sciences, Michigan Technological University, Houghton, MI 49931 USA (email: yfujiwar@mtu.edu; tonchev@mtu.edu).

A *difference system of sets* (DSS) of index ρ over \mathbf{Z}_v is a family of disjoint subsets Q_i of \mathbf{Z}_v such that the multi-set

$$\{a - b \pmod{v} \mid a \in Q_i, b \in Q_j, i \neq j\} \quad (1)$$

contains every $d \in \mathbf{Z}_v \setminus \{0\}$ at least ρ times. The difference between two elements from different subsets of \mathbf{Z}_v is called an *outer difference*. A DSS is *perfect* if the multi-set (refequ) contains every $d \in \mathbf{Z}_v \setminus \{0\}$ exactly ρ times. A DSS is *regular* if all subsets Q_i are of the same size. A regular DSS that consists of q subsets of cardinality m is denoted by $\text{DSS}(v, m, q, \rho)$.

DSSs were introduced to realize self-synchronizing codes as cosets of linear codes in order to achieve low encoding and decoding complexity [27], [28]. Regardless of which error-correcting code we use to protect the payload we transmit, a DSS of index ρ assures self-synchronization under the presence of up to $\lfloor \frac{\rho-1}{2} \rfloor$ symbol substitutions (or errors) in the received message of length v . Various construction methods for DSSs have been developed in recent years. For the latest results and a survey of earlier research, we refer the reader to [15], [36], [45] and references therein.

Of particular interest are DSSs that require fewer bits for self-synchronization. The number of bits required for synchronization is exactly the number of elements used in the DSS, that is, $|Q_0 \cup Q_1 \cup \dots \cup Q_{q-1}|$. All the remaining bits may freely be used for information transmission. For example, a regular $\text{DSS}(v, m, q, \rho)$ generates a self-synchronizing code of index ρ with $v - mq$ information bits. The cardinality $|Q_0 \cup Q_1 \cup \dots \cup Q_{q-1}|$ is called the *redundancy* of the DSS. The minimum redundancy for given v, q , and ρ is denoted by $r_q(v, \rho)$. Levenshtein [27] proved the following lower bound on $r_q(v, \rho)$:

$$r_q(v, \rho) \geq \sqrt{\frac{q\rho(v-1)}{(q-1)}} \quad (2)$$

with equality if and only if the DSS is perfect and regular. A sharper bound was proved by Wang [38]:

$$r_q(v, \rho) \geq \sqrt{S(\rho(v-1) + \left\lceil \frac{\rho(v-1)}{(q-1)} \right\rceil)}$$

where $S(n)$ denotes the smallest square number that is greater than or equal to n .

A DSS is *optimal* if its redundancy is the lowest possible for given parameters. If the redundancy of an infinite series of DSSs approaches a known lower bound as some other parameters tend to infinity, we say such DSSs are *asymptotically optimal*.

Equally important, or perhaps more important in practical situations, is the ratio of the number of bits allocated for self-synchronization to the number of bits available for information

transmission. In the case of a self-synchronizing code obtained from a DSS, the *redundancy rate* of a DSS over \mathbf{Z}_v using s symbols is defined as the fraction $e = \frac{s}{v}$. For instance, the redundancy rate of a regular DSS(v, m, q, ρ) is $\frac{mq}{v}$. A DSS of redundancy rate e gives a self-synchronizing code of constant code length v where ev bits of each codeword are used for self-synchronization. Clearly the information rates of the corresponding self-synchronization codes depend not on the optimality of DSSs, but on the absolute values of the redundancy rates. For instance, a DSS that leaves only one bit for information transmission can still be judged as “optimal” with respect to Inequality (2). In other words, optimality means something only when the target information rate is met.

While nontrivial DSSs are of interest and may allow us to realize self-synchronizing codes as cosets of linear codes, it seems quite difficult to construct such combinatorial objects. A particularly difficult task is to suppress redundancy rates to a very low level. In fact, optimal or asymptotically optimal DSSs with redundancy rates significantly lower than a half are quite rare; if we use a DSS of redundancy rate, say, $\frac{2}{3}$, we must sacrifice two thirds of the bits for self-synchronization, regardless of whether it is optimal or not. While DSSs with high redundancy rates are certainly of mathematical interest (see, for example, [1], [2], [10], [17], [18], [21], [34], [36] for relations to other mathematical concepts), one has to sacrifice a significant portion of bits just for synchronization.

The primary purpose of this paper is to propose a simple remedy for this information rate problem. We give simple combinatorial methods for constructing DSSs with lower redundancy rates from ones with higher redundancy rates, allowing for self-synchronizing codes with improved information rates. Our methods give asymptotically optimal DSSs with low redundancy rates when applied to carefully chosen ingredients. The redundancy rate of one of our low redundancy DSSs reaches about $\frac{1}{72}$, which, as far as the authors are aware, is a level that has never been achieved by any known optimal or asymptotically optimal DSS with high error-tolerance. We also present direct constructions for optimal DSSs that are suited for use as ingredients of our redundancy reduction methods.

II. PRODUCT CONSTRUCTIONS

In this section, we give combinatorial constructions that generate difference systems of sets of lower redundancy rate from those with higher redundancy rates. For the sake of simplicity, for the most part we use perfect regular DSSs as ingredients to derive new DSSs. The constructions can generate various infinite classes of difference systems of sets including asymptotically optimal ones. The same technique is applicable to any DSS that may or may not be perfect or regular in a straightforward manner.

To make it easier to see the mechanism of the redundancy reduction process, we first give a simpler construction for DSSs¹ and demonstrate how to use it to reduce the redundancy

rates of known DSSs. A generalized version of the construction is then presented.

Let \mathcal{P} be a family of subsets B_0, B_1, \dots, B_{q-1} of size m over \mathbf{Z}_v . The family \mathcal{P} is said to form a *difference family* over \mathbf{Z}_v and is denoted by $\text{DF}(v, m, \lambda)$ if every nonzero element of \mathbf{Z}_v appears exactly λ times in the multi-set $\{a - b \mid a, b \in B_i, 0 \leq i \leq q - 1\}$. A difference family can be defined the same way when \mathcal{P} may contain subsets of different cardinalities. If the subset sizes are not uniform, we specify possible sizes by the set $K = \{|B_i| \mid 0 \leq i \leq q - 1\}$ and write $\text{DF}(v, K, \lambda)$. When all B_i are of size one, \mathcal{P} is a cyclic *difference set* and written as $\text{DS}(v, m, \lambda)$. As opposed to outer differences, a difference between elements of the same set is called an *inner difference*. Roughly speaking, a DF is an inner version of a perfect DSS in the sense that the number of occurrences of each inner difference in a DF is uniform across all the nonzero elements while in a perfect DSS outer differences occur uniformly.

Theorem 2.1: Let v and v' be relatively prime positive integers. If there exist a perfect regular DSS(v, m, q, ρ) forming a $\text{DF}(v, m, \lambda)$ and a perfect regular DSS(v', m', q', ρ') forming a $\text{DF}(v', m', \lambda')$, then there exists a regular DSS($vv', mm', qq', \min(\rho\rho' + \rho\lambda' + \rho'\lambda, \rho m'q', \rho'mq)$).

Proof: Let $\mathcal{A} = \{Q_0, Q_1, \dots, Q_{q-1}\}$ and $\mathcal{B} = \{Q'_0, Q'_1, \dots, Q'_{q'-1}\}$ be a perfect regular DSS(v, m, q, ρ) forming a $\text{DF}(v, m, \lambda)$ and a perfect regular DSS(v', m', q', ρ') forming a $\text{DF}(v', m', \lambda')$ respectively. Take family

$$\mathcal{C} = \{Q_i \times Q'_j \mid 0 \leq i \leq q - 1, 0 \leq j \leq q' - 1\}$$

of all the direct products between elements of \mathcal{A} and those of \mathcal{B} . Since v and v' are relatively prime, \mathcal{C} can be seen as a family of qq' disjoint sets of size mm' over $\mathbf{Z}_{vv'}$. It suffices to prove that each outer difference appears either $\rho\rho' + \rho\lambda' + \rho'\lambda$, $\rho m'q'$ or $\rho'mq$ times.

Write an element of the cyclic group of order vv' as (a, b) where $a \in \mathbf{Z}_v$ and $b \in \mathbf{Z}_{v'}$. Since \mathcal{A} is a family of disjoint sets, an outer difference of the form $(0, b)$ only occurs between $Q_i \times Q'_j$ and $Q_i \times Q'_k$ for some j and k . Assume that Q'_j and Q'_k give b as an outer difference exactly $x(j, k)$ times. For every i , $0 \leq i \leq q - 1$, and fixed j and k , there are $m \cdot x(j, k)$ instances of outer difference $(0, b)$ between $Q_i \times Q'_j$ and $Q_i \times Q'_k$. Since \mathcal{B} is a DSS of index ρ' , taking all possible pairs Q'_j and Q'_k gives ρ' instances of b as an outer difference. Hence, we have

$$\sum_i \sum_{j, k} m \cdot x(j, k) = \rho' m q.$$

Hence, we have each outer difference of the form $(0, b)$ exactly $\rho' m q$ times in \mathcal{C} . By the same token, each outer difference of the form $(a, 0)$ occurs exactly $\rho m' q'$ times.

Consider an outer difference of the form (a, b) with $a, b \neq 0$. We first consider outer differences between $Q_i \times Q'_j$ and $Q_i \times Q'_k$ with $j \neq k$. Since \mathcal{A} is a $\text{DF}(v, m, \lambda)$, inner difference a occurs exactly λ times in \mathcal{A} . For each occurrence, taking all possible j and k gives ρ' instances of outer difference (a, b) . Hence, for fixed a and b , we have (a, b) as an outer difference exactly $\rho'\lambda$ times between $Q_i \times Q'_j$ and $Q_i \times Q'_k$ with $j \neq k$. Similarly, we have $\rho\lambda'$ (a, b) s between $Q_i \times Q'_j$ and $Q_k \times Q'_j$

¹Essentially the same construction appeared without proof in the context of combinatorics of outer differences in a workshop abstract by the first author and Fuji-Hara [19] (see also [39]). Here we give a complete proof and explain how this technique improves information rates in the context of self-synchronizing codes.

with $i \neq k$. Consider outer differences between $Q_i \times Q'_j$ and $Q_k \times Q'_l$ with $i \neq k$ and $j \neq l$. Since \mathcal{A} and \mathcal{B} are DSSs of indices ρ and ρ' respectively, it is straightforward to see that by taking all possible i, j, k, l , we get (a, b) exactly $\rho\rho'$ times between $Q_i \times Q'_j$ and $Q_k \times Q'_l$ with $i \neq k$ and $j \neq l$. Hence we have each outer difference of the form (a, b) with $a, b \neq 0$ exactly $\rho\rho' + \rho\lambda' + \rho'\lambda$ times. The proof is complete. ■

Note that the redundancy rate of the resulting DSS is the product between those of the DSSs used as ingredients. Because redundancy rates are always less than or equal to 1 for any DSSs, the resulting DSS always has a lower or equal redundancy rates when compared to the ingredients, which means that the corresponding self-synchronizing code can take advantage of more information bits. It is also worth noting that the same technique can be applied to DSSs that do not form difference families, albeit with a more complicated analysis of the number of occurrences of each inner and outer difference.

The direct product technique described above can give infinitely many series of asymptotically optimal regular difference systems of sets. The following is an example of an infinite class of such DSSs obtained from the ones of Paley type (see [35]):

Corollary 2.2: Let v and v' be two distinct primes congruent to 3 modulo 4 and write $v = 2mq + 1$ and $v' = 2m'q' + 1$ for some positive integers m, m', q , and q' respectively. Then there exists an asymptotically optimal class of regular DSSs of parameters $(vv', mm', qq', \frac{m(m'-1)(q-1)+(m-1)m'(q'-1)+mm'(q-1)(q'-1)}{4})$.

Proof: Let v and v' be two distinct primes congruent to 3 modulo 4 as stated in the statement. Then there exist perfect regular DSSs of parameters $(v, m, q, \frac{v-2m-1}{4})$ and $(v', m', q', \frac{v'-2m'-1}{4})$ which form DFs of indices $\lambda = \frac{v-1}{4}$ and $\lambda' = \frac{v'-1}{4}$ respectively [35]. Let $\rho = \frac{v-2m-1}{4}$ and $\rho' = \frac{v'-2m'-1}{4}$. A simple calculation of the comma index shows that $\min(\rho\rho' + \rho\lambda' + \rho'\lambda, \rho m'q', \rho' m q) = \rho\rho' + \rho\lambda' + \rho'\lambda = \frac{m(m'-1)(q-1)+(m-1)m'(q'-1)+mm'(q-1)(q'-1)}{4}$. Applying Theorem 2.1 gives a perfect regular DSS of the desired parameters. Observing Inequality (2), it is straightforward to show that

$$\lim_{m, m' \rightarrow \infty} \frac{r_{qq'}(vv', \rho\rho' + \rho\lambda' + \rho'\lambda)}{mm'qq'} = 1.$$

The proof is complete. ■

The asymptotically optimal DSSs allow for greatly improved information rates compared to the ingredient systems. In fact, the redundancy rate of a DSS obtained from Corollary 2.2 is only $\frac{(v-1)(v'-1)}{4vv'} \approx \frac{1}{4}$ while that of the Paley type DSSs is $\frac{v-1}{2v} \approx \frac{1}{2}$.

The redundancy rate of the resulting DSSs in Theorem 2.1 depend on ingredient systems. Hence, direct constructions of DSSs having low redundancy rates are important in constructing a DSS with very low redundancy rates. Among many results in the literature, optimal perfect regular DSSs with remarkably low redundancy rates were given in [18] by partitioning the points of hyperplanes of projective spaces:

Theorem 2.3 ([18]): There exists a partition of the points of a hyperplane of the projective space $\text{PG}(2s, p)$ into an optimal perfect regular DSS $(\frac{p^{2s+1}-1}{p-1}, p+1, \frac{p^{2s}-1}{p^2-1}, \frac{p^{2s-1}-p}{p-1})$ forming

a DF $(\frac{p^{2s+1}-1}{p-1}, p+1, 1)$ for $p = 2$ and $s \leq 5$, $p = 3$ and $s \leq 3$, and $p = 5, 8, 9$ and $s = 2$.

For example, the redundancy rates of their DSS from $\text{PG}(4, 9)$ is $\frac{9^4-1}{9^5-1} \approx \frac{1}{9}$. Theorem 2.1 can lower this rate even further. For instance, we can reduce the redundancy rate to approximately $\frac{1}{72}$ by applying the direct product technique with the DSS from $\text{PG}(4, 8)$.

Corollary 2.4: Let p and s be positive integers satisfying $p = 2$ and $s \leq 5$, $p = 3$ and $s \leq 3$ or $p = 5, 8, 9$ and $s = 2$. Take one more pair p' and s' of integers satisfying the same condition. If $\gcd(\frac{p^{2s+1}-1}{p-1}, \frac{p'^{2s'+1}-1}{p'-1}) = 1$, then there exists a regular DSS $(\frac{(p^{2s+1}-1)(p'^{2s'+1}-1)}{(p-1)(p'-1)}, (p+1)(p'+1), \frac{(p^{2s}-1)(p'^{2s'}-1)}{(p^2-1)(p'^2-1)}, \frac{(p^{2s-1}-p)(p'^{2s'-1}-p')}{(p-1)(p'-1)})$.

Proof: Apply Theorem 2.1 to Theorem 2.3. The assertion follows from a simple calculation. ■

We now generalize the construction technique used in Theorem 2.1. The previous construction requires that the lengths of the pair of self-synchronizing codes corresponding to the DSSs used as ingredients be relatively prime. We relax this condition by using a combinatorial technique similar to the one found in [12]. Unlike the simpler construction, the generalized version does not simply take the direct product between two sets from a pair of DSSs. To avoid unduly involved technical arguments and succinctly present the combinatorics behind the key idea, we restrict one ingredient to a DSS of redundancy rate one. Such DSSs are equivalent to frequency hopping patterns for spread-spectrum multiple access communications. More formally, a *frequency hopping sequence* of period v over a set F of cardinality q is a v -dimensional vector $X = (x_0, x_1, \dots, x_{v-1})$ with $x_i \in F$ for $0 \leq i \leq v-1$, where $|F| = q$. By taking the support of each element of F , we obtain q disjoint subsets partitioning the set $\{0, 1, \dots, v-1\}$, which can be seen as a DSS of certain index.

One objective of the study of frequency hopping sequences is to minimize the number of occurrences of each inner difference for given v and q , or equivalently, to minimize the off-peak Hamming autocorrelations for given v and q (see [16]). It is straightforward to see that the sum of the number of occurrences of inner difference i and that of outer difference i is v . Hence, a DSS of index ρ and redundancy rate one is equivalent to a frequency hopping sequence in which each inner difference appears at most $v - \rho$ times. In what follows, we write a DSS of length v , index ρ , and redundancy rate one on q sets as FHS $(v, v - \rho; q)$.

Theorem 2.5: If there exist an FHS $(v, v - \rho; q)$ and a perfect DSS of length v' , index ρ' , and redundancy rate e' forming a DF (v', K, λ') , then there exists a DSS of length vv' , index $\min(\rho e' v', v(\lambda' + \rho'))$, and redundancy rate e' on $qv'e'$ sets.

Proof: Let $\mathcal{A} = \{Q_0, Q_1, \dots, Q_{q-1}\}$ and $\mathcal{B} = \{Q'_0, Q'_1, \dots, Q'_{q'-1}\}$ be an FHS $(v, v - \rho; q)$ and a DSS with the parameters given in the statement respectively. We write the elements of the rings \mathbf{Z}_v and $\mathbf{Z}_{v'}$ by $\{0, 1, \dots, v-1\}$ and $\{0, 1, \dots, v'-1\}$ respectively. We construct subsets of $\mathbf{Z}_{vv'}$ by embedding the elements of the two rings. For every Q_i and $x \in \bigcup_j Q'_j$, define the set $S_{i,x} = \{v'a + x \mid a \in Q_i\}$ over

$\mathbf{Z}_{vv'}$. Let

$$\mathcal{S} = \left\{ S_{i,x} \mid 0 \leq i \leq q-1, x \in \bigcup_j Q'_j \right\}.$$

\mathcal{S} is a family of disjoint $qv'e'$ subsets of $\mathbf{Z}_{vv'}$. We have $|\bigcup S_{i,x}| = e'vv'$. It suffices to prove that each outer difference in \mathcal{S} appears at least $\min(\rho e'v', v(\lambda' + \rho'))$ times.

An outer difference that is divisible by v' appears at least ρ times between $S_{i,x}$ and $S_{j,x}$. Because there are $v'e'$ choices for x , the number of occurrences of an outer difference of this kind is at least $\rho v'e'$. An outer difference that is not divisible by v' appears exactly $\lambda'v$ times between $S_{i,x}$ and $S_{j,y}$ for $x, y \in Q'_k$, and $\rho'v$ times between $S_{i,x}$ and $S_{j,y}$ for $x \in Q'_k, y \in Q'_l$ with $k \neq l$. Hence, the total number of occurrences is $v(\lambda' + \rho')$. The proof is complete. ■

Frequency hopping sequences have extensively been studied from various viewpoints. Constructions for frequency hopping sequences with optimal Hamming autocorrelations can be found in [3], [5]–[7], [13], [16], [20], [22]–[24], [26], [37], [43]. Known constructions for sets of frequency hopping sequences may be used for Theorem 2.5 as well because each set contains frequency hopping sequences with good Hamming autocorrelations (see [41], [44] for recent results). Equivalent or closely related mathematical objects have also been investigated under the names of constant composition codes [4], [14], [30] (see also [29], [46] for more details and the latest results), partition difference families [25], [40], [42], external difference families [1], and zero-difference balanced functions [11], [45].

In the reminder of this section, we briefly look into what kind of DSS can be obtained through the technique used in Theorem 2.5.

As in Theorem 2.1, the redundancy rate of the resulting difference system of sets generated by the technique given in the proof of Theorem 2.5 is the product of the redundancy rates of the two ingredients. Hence, a DSS of extremely high redundancy rate will not lead to a significantly improved information rate. In this sense, it is important to utilize at least one DSS of low redundancy rate as an ingredient. Nonetheless, a frequency hopping sequence, which is a DSS that uses up all bits, can still be used to obtain DSSs of very good or even optimal redundancy with respect to Inequality (2). In fact, Theorem 4 in [39] can be seen as a corollary of Theorem 2.5:

Corollary 2.6: If there exist an FHS($v, v - \rho; q$) and a DS(v', m', λ'), then there exists a DSS of length vv' , index $\min(\rho m', v\lambda')$, and redundancy rate $\frac{m'}{v'}$ based on qm' sets.

Proof: A DS(v', m', λ') is also a perfect regular DSS($v', m', 1, 0$) forming a DF(v', m', λ'). Applying Theorem 2.5 proves the assertion. ■

Difference sets are important combinatorial objects and have been a topic of extensive research [8]. To see how good the DSSs of Corollary 2.6 are in terms of optimality, take, for example, the projective plane over the finite field of order k as a DS($k(k-1)+1, k, 1$). If we fix the FHS($v, v-\rho; q$) used as an ingredient, the index of the resulting DSS is $\min(\rho k, v) = v$ for large k . The ratio between the redundancy of the resulting

DSS and the righthand side of Inequality (2) approaches 1 as k tends to infinity. Hence, we obtain an infinite series of asymptotically optimal DSSs. The construction process of the optimal DSS of length 49 and redundancy rate $\frac{3}{7}$ given in Example 5 of [39] can be seen as an application of the Fano plane to Corollary 2.6.

In general, the product techniques degrade optimality only slightly if at all if ingredients are chosen so that every outer difference appears almost uniformly in the resulting DSS. One possible drawback of the product constructions is that the code length is inherently longer than those of the codes used as ingredients. This implies that a high-rate self-synchronizing code of very short length is difficult to obtain by our approach. Another limitation to the available lengths is that they must be composite numbers, which can be a problem if one wishes a code of prime length. The increased alphabet size may also be of concern if one would like to employ self-synchronizing codes in a q -nary system with very small q . We deal with these problems in the following section by giving direct constructions for binary and ternary DSSs of prime lengths.

III. CYCLOTOMIC CONSTRUCTIONS

To take advantage of the techniques presented in the previous section, we need difference systems of sets with good parameters to start with. In the context of improving information rates, generally speaking, DSSs with low redundancy rates are desirable as ingredients. Perfect regular DSSs are particularly suited for this task because they make it easier to calculate the parameters of the resulting DSSs while ensuring low redundancy due to the optimality that comes from the fact that the equality in (2) holds if and only if a DSS is simultaneously perfect and regular.

In this section we give perfect regular DSSs of redundancy rate less than $\frac{1}{2}$. To this end, we revisit a known direct construction for DSSs based on cyclotomy [33]. Although it is known that DSSs of various types and parameters can be constructed in a similar manner [31]², to keep clarity and simplicity of our approach, we focus on the kind of DSS that is particularly suited for our purpose and do not deal with DSSs that would be too cumbersome to apply to the product constructions.

Let $p = fm + 1$ be an odd prime for some positive integers f and m . The f th cyclotomic classes in \mathbb{F}_p are defined as $C_i^f = \{\alpha^{i+tf} \mid 0 \leq t \leq m-1\}$, where α is a primitive element of \mathbb{F}_p and $0 \leq i \leq f-1$. The cyclotomic numbers of order f are $(i, j)_f = |(C_i + 1) \cup C_j|$. We use the following theorem:

Theorem 3.1 ([33]): Let $p = fmq + 1$ be an odd prime, where f, m , and q are positive integers. The family $\{C_{fi}^{fq} \mid 0 \leq i \leq q-1\}$ of cyclotomic classes is a regular DSS(p, m, q, ρ), where

$$\rho = \min \left(\sum_{j=0}^{q-1} \sum_{a=1}^{q-1} (i + jf, af)_{fq} \mid 0 \leq i \leq f-1 \right).$$

²In fact, the constructions given in this section may be regarded as special cases of the results reported in an unpublished manuscript [32].

In particular, if

$$\sum_{j=0}^{q-1} \sum_{a=1}^{q-1} (i + jf, af)_{fq} = \frac{m(q-1)}{f}$$

for every i , then the regular DSS is of index $\frac{m(q-1)}{f}$, perfect, and hence optimal.

Note that Theorem 3.1 was originally stated in a slightly different way. A simple calculation of cyclotomic numbers gives the above form.

A few sporadic examples of perfect regular DSSs were found through Theorem 3.1 [33]. Our key observation here is that in some cases it is readily checked whether the condition

$$\sum_{j=0}^{q-1} \sum_{a=1}^{q-1} (i + jf, af)_{fq} = \frac{m(q-1)}{f}$$

for every i holds, so that the cyclotomic construction can give a series of perfect regular DSSs with low redundancy rates.

Theorem 3.2: For every n such that $16n^2 + 1$ is an odd prime, there exists a perfect regular DSS($16n^2 + 1, 4n^2, 2, 2n^2$).

Proof: Assume that $16n^2 + 1$ is an odd prime. Take C_0^4 and C_2^4 . Because $\frac{(16n^2+1)-1}{4} = 4n^2$ is even, by the classic result on cyclotomic numbers for when the order is a small divisor of $p-1$, p prime [9], we have

$$\begin{aligned} (0, 2)_4 + (2, 2)_4 &= 2(0, 2)_4 \\ &= \frac{16n^2 + 1 - 3 + 2}{8} \\ &= 2n^2 \end{aligned}$$

and

$$\begin{aligned} (1, 2)_4 + (3, 2)_4 &= 2(1, 2)_4 \\ &= \frac{16n^2 + 1 + 1 - 2}{8} \\ &= 2n^2. \end{aligned}$$

Thus, we have

$$\begin{aligned} (0, 2)_4 + (2, 2)_4 &= (1, 2)_4 + (3, 2)_4 \\ &= 2n^2 \\ &= \frac{4n^2(2-1)}{2}. \end{aligned}$$

Applying Theorem 3.1 completes the proof. \blacksquare

Because the DSSs in Theorem 3.2 are both perfect and regular, they are optimal. The redundancy rate is $\frac{8n^2}{16n^2+1} \approx \frac{1}{2}$.

This technique works for primes of other similar forms as well. Here we give two more example series of perfect regular DSSs, one of which gives redundancy rate about $\frac{1}{2}$ and the other about $\frac{1}{3}$. The former generates optimal ternary DSSs, and the latter binary.

Theorem 3.3: For every n such that $12n^2 + 1$ is an odd prime, there exists a perfect regular DSS($12n^2 + 1, 2n^2, 3, 2n^2$).

Proof: Take positive integer n such that $12n^2 + 1$ is an odd prime. Take C_0^6 , C_2^6 , and C_4^6 . By the same argument as

in the proof of Theorem 3.2, we have

$$\begin{aligned} \sum_{j=0}^2 \sum_{a=1}^2 (0 + 2j, 2a)_6 &= (0, 2)_6 + (0, 4)_6 + (2, 4)_6 \\ &= \frac{12n^2 + 1 - 3 + 2}{6} \\ &= 2n^2 \end{aligned}$$

and

$$\begin{aligned} \sum_{j=0}^2 \sum_{a=1}^2 (1 + 2j, 2a)_6 &= (1, 2)_6 + (1, 3)_6 + (1, 4)_6 \\ &= \frac{12n^2 + 1 + 1 - 2}{6} \\ &= 2n^2. \end{aligned}$$

Hence, by Theorem 3.1 the cyclotomic classes form a perfect regular DSS as desired. \blacksquare

Theorem 3.4: For every n such that $108n^2 + 1$ is an odd prime, there exists a perfect regular DSS($108n^2 + 1, 18n^2, 2, 6n^2$).

Proof: Let $p = 108n^2 + 1$ be an odd prime. Take C_0^6 and C_3^6 . Because 2 is a cubic residue of p , as in the proofs of the previous two theorems, we have

$$(i, 3)_6 + (i + 3, 3)_6 = \frac{18n^2(2-1)}{3}$$

for $i = 0, 1$. \blacksquare

Whether Theorems 3.2, 3.3, and 3.4 are infinite series of optimal DSSs depends on whether there exist infinitely many primes of the form $an^2 + b$ for given a and b . The simplest case when $a = b = 1$ is already a notoriously difficult problem, known as Landau's problem, which has been open for a hundred years.

DSSs given in this section are optimal and have very small q and relatively low redundancy rates. Theorem 3.1 can give many more perfect and almost perfect DSSs in a similar way by computing cyclotomic numbers. If one wishes to further reduce redundancy rates by the product constructions, the comma-free indices of the resulting DSSs can be calculated by the indices of the ingredients and the number $\min_i \left(\sum_{j=0}^{q-1} (i + jf)_{fq} \right)$ of appearances of the least frequent inner difference in each ingredient (see [33]). Hence, while it seems impossible to give a simple and general formula for the exact values of the parameters of the resulting DSSs obtained in this manner, calculating them for each individual case is relatively easy.

IV. CONCLUSION

We have developed simple combinatorial methods for reducing the redundancy rates of difference systems of sets while sacrificing optimality to only a small extent. In fact, our product constructions give asymptotically optimal DSSs when applied to carefully chosen optimal DSSs. This gives a simple remedy for the problem that even optimal DSSs may end up using a significant portion of bits which otherwise could be used for information transmission. Our methods hence improve the information rate of communications while allowing

for a systematic construction for self-synchronizing codes of low redundancy. To take full advantage of and complement our methods, we also constructed perfect regular DSSs with low redundancy rates directly through cyclotomy. While we focused on the kind of DSS that can not be obtained through the product constructions and is useful for our approach to improving information rates, the cyclotomic construction can give various series of regular DSSs with excellent redundancy that are of interesting on their own. A further look into this type of construction would be interesting.

As far as the authors are aware, the result presented here is the first mathematical approach that draws attention to systematically lowering the redundancy rates of DSSs and improving the information rates of the corresponding self-synchronizing codes. Because the absolute values of redundancy rates are as important as optimality, we believe that further investigations into redundancy rates are needed from both mathematical and coding theoretic viewpoints.

ACKNOWLEDGMENT

The authors thank Yukiyasu Mutoh for sharing his unpublished manuscript [32]. This research was conducted while the first author was visiting the Department of Mathematical Sciences, Michigan Technological University. He thanks the department for the hospitality.

REFERENCES

- [1] Y. Chang and C. Ding, "Constructions of external difference families and disjoint difference families," *Des. Codes Cryptogr.*, vol. 49, pp. 167–185, 2006.
- [2] Y. M. Chee, A. C. H. Ling, and J. Yin, "Optimal partitioned cyclic difference packings for frequency hopping and code synchronization," *IEEE Trans. Inf. Theory*, vol. 56, pp. 5738–5746, 2010.
- [3] W. Chu and C. J. Colbourn, "Optimal frequency-hopping sequences via cyclotomy," *IEEE Trans. Inf. Theory*, vol. 51, pp. 1139–1141, 2005.
- [4] W. Chu, C. J. Colbourn, and P. Dukes, "On constant composition codes," *Discrete Appl. Math.*, vol. 154, pp. 912–929, 2006.
- [5] J.-H. Chung, Y. K. Han, and K. Yang, "New classes of optimal frequency-hopping sequences by interleaving techniques," *IEEE Trans. Inf. Theory*, vol. 55, pp. 5783–5791, 2009.
- [6] J.-H. Chung and K. Yang, "Optimal frequency-hopping sequences with new parameters," *IEEE Trans. Inf. Theory*, vol. 56, pp. 1685–1693, 2010.
- [7] J.-H. Chung and K. Yang, " k -Fold cyclotomy and its application to frequency-hopping sequences," *IEEE Trans. Inf. Theory*, vol. 57, pp. 2306–2317, 2011.
- [8] C. J. Colbourn and J. H. Dinitz, Eds., *Handbook of Combinatorial Designs*, 2nd ed. Boca Raton, FL: Chapman & Hall/CRC, 2007.
- [9] L. E. Dickson, "Cyclotomy, higher congruences, and Waring's problem," *Amer. J. Math.*, vol. 57, pp. 391–424, 1935.
- [10] C. Ding, "Optimal and perfect difference systems of sets," *J. Combin. Theory Ser. A*, vol. 116, pp. 109–119, 2008.
- [11] C. Ding, "Optimal constant composition codes from zero-difference balanced functions," *IEEE Trans. Inf. Theory*, vol. 54, pp. 5766–5770, 2008.
- [12] C. Ding, R. Fuji-Hara, Y. Fujiwara, M. Jimbo, and M. Mishima, "Sets of frequency hopping sequences: bounds and optimal constructions," *IEEE Trans. Inf. Theory*, vol. 55, pp. 3297–3304, 2009.
- [13] C. Ding, M. Miosio, and J. Yuan, "Algebraic constructions of optimal frequency hopping sequences," *IEEE Trans. Inf. Theory*, vol. 53, pp. 2606–2610, 2007.
- [14] C. Ding and J. Yin, "Combinatorial constructions of optimal constant composition codes," *IEEE Trans. Inf. Theory*, vol. 51, pp. 3671–3673, 2005.
- [15] C.-L. Fan and J.-G. Lei, "Constructions of difference systems of sets from finite projective geometry," *IEEE Trans. Inf. Theory*, vol. 58, no. 1, pp. 130–138, 2012.
- [16] R. Fuji-Hara, Y. Miao, and M. Mishima, "Optimal frequency hopping sequences: A combinatorial approach," *IEEE Trans. Inf. Theory*, vol. 50, pp. 1408–2420, 2004.
- [17] R. Fuji-Hara, K. Momihara, and M. Yamada, "Perfect difference systems of sets and jacobi sums," *Discrete Math.*, vol. 309, pp. 3954–3961, 2009.
- [18] R. Fuji-Hara, A. Munemasa, and V. D. Tonchev, "Hyperplane partitions and difference systems of sets," *J. Combin. Theory Ser. A*, vol. 113, pp. 1699–1718, 2006.
- [19] Y. Fujiwara and R. Fuji-Hara, "Frequency hopping sequences with optimal auto- and cross-correlation properties and related codes," in *Proc. Tenth Int. Workshop Algebraic and Combin. Coding Theory*, vol. 10, 2006, pp. 93–96.
- [20] G. Ge, R. Fuji-Hara, and Y. Miao, "Further combinatorial constructions for optimal frequency hopping sequences," *J. Combin. Theory Ser. A*, vol. 113, pp. 1699–1718, 2006.
- [21] G. Ge, Y. Miao, and L. Wang, "Combinatorial constructions for optimal splitting authentication codes," *SIAM J. Discrete Math.*, vol. 18, pp. 663–678, 2005.
- [22] Y. K. Han and K. Yang, "On the Sidelnikov sequences as frequency-hopping sequences," *IEEE Trans. Inf. Theory*, vol. 55, pp. 4279–4285, 2009.
- [23] J. J. Komo and S. C. Liu, "Maximal length sequences for frequency hopping," *IEEE J. Sel. Areas Commun.*, vol. 5, pp. 819–822, 1990.
- [24] P. V. Kumar, "Frequency-hopping code sequence designs having large linear span," *IEEE Trans. Inf. Theory*, vol. 34, pp. 146–151, 1988.
- [25] J. Lei and C. Fan, "Optimal difference systems of sets and partition-type cyclic difference packings," *Des. Codes Cryptogr.*, vol. 58, pp. 135–153, 2011.
- [26] A. Lempel and H. Greenberger, "Families of sequences with optimal hamming correlation properties," *IEEE Trans. Inf. Theory*, vol. 20, pp. 90–94, 1974.
- [27] V. I. Levenshtein, "One method of constructing quasi codes providing synchronization in the presence of errors," *Problems Inform. Transmission*, vol. 7, no. 3, pp. 215–222, 1971.
- [28] V. I. Levenshtein, "Combinatorial problems motivated by comma-free codes," *J. Combin. Des.*, vol. 12, pp. 184–196, 2004.
- [29] J. Luo and T. Hellesteth, "Constant composition codes as subcodes of cyclic codes," *IEEE Trans. Inf. Theory*, vol. 57, pp. 7482–7488, 2011.
- [30] Y. Luo, F. W. Fu, A. J. Han Vinck, and W. Chen, "On constant composition codes over \mathbb{Z}_p ," *IEEE Trans. Inf. Theory*, vol. 49, pp. 3010–3016, 2003.
- [31] Y. Mutoh, *Private communication*.
- [32] Y. Mutoh, "Difference systems of sets and cyclotomy II," *Unpublished manuscript*.
- [33] Y. Mutoh and V. D. Tonchev, "Difference systems of sets and cyclotomy," *Discrete Math.*, vol. 308, pp. 2959–2969, 2008.
- [34] W. Ogata, K. Kurosawa, D. R. Stinson, and H. Saido, "New combinatorial designs and their applications to authentication codes and secret sharing schemes," *Discrete Math.*, vol. 279, pp. 383–405, 2004.
- [35] V. D. Tonchev, "Difference systems of sets and code synchronization," *Rendiconti del Seminario Matematico di Messina Series II*, vol. 9, pp. 217–226, 2003.
- [36] V. D. Tonchev, "Partitions of difference sets and code synchronization," *Finite Fields Appl.*, vol. 11, pp. 601–621, 2005.
- [37] P. Udaya and M. N. Siddiqi, "Optimal large linear complexity frequency hopping patterns derived from polynomial residue class rings," *IEEE Trans. Inf. Theory*, vol. 44, pp. 1492–1503, 1998.
- [38] H. Wang, "A new bound for difference systems of sets," *J. Combin. Math. Combin. Comput.*, vol. 58, pp. 161–168, 2006.
- [39] X. Wang and J. Wang, "Optimal difference systems of sets and difference sets," *Aequat. Math.*, vol. 82, pp. 155–164, 2011.
- [40] X. Wang and J. Wang, "Partitioned difference families and almost difference sets," *J. Statist. Plann. Infer.*, vol. 141, pp. 1899–1909, 2011.
- [41] Y. Yang, X. Tang, U. Parampalli, and D. Peng, "New bound on frequency hopping sequence sets and its optimal constructions," *IEEE Trans. Inf. Theory*, vol. 57, pp. 7605–7613, 2011.
- [42] J. Yin, X. Shan, and Z. Tian, "Constructions of partitioned difference families," *European J. Combin.*, vol. 29, pp. 1507–1519, 2008.
- [43] X. Zeng, H. Cai, X. Tang, and Y. Yang, "A class of optimal frequency hopping sequences with new parameters," *IEEE Trans. Inf. Theory*, vol. 58, pp. 4899–4907, 2012.
- [44] Z. Zhou, X. Tang, D. Peng, and U. Parampalli, "New constructions for optimal sets of frequency-hopping sequences," *IEEE Trans. Inf. Theory*, vol. 57, pp. 3831–3840, 2011.
- [45] Z. Zhou, X. Tang, D. Wu, and Y. Yang, "Some new classes of zero-difference balanced functions," *IEEE Trans. Inf. Theory*, vol. 58, pp. 139–145, 2012.

- [46] M. Zhu and G. Ge, “Quaternary constant-composition codes with weight four and distances five or six,” *IEEE Trans. Inf. Theory*, 2012, to appear.